REMARKS/ARGUMENTS

In the Office action dated August 31, 2005, the Examiner raised objections to the claims, and rejected claims 1 - 10 and 26 - 40 under 35 U.S.C. § 103. By this Amendment, Applicant has amended claims 4, 7, 32 and 37 and added claims 41 - 45. Reconsideration and reexamination are hereby requested for claims 1 - 10 and 26 - 45 that are now pending in this application.

Response to the Objection to the Claims

The Examiner objected to claims 4, 7 and 37 because of various informalities. Applicant has amended the claims as suggested by the Examiner.

Response to the 35 U.S.C. § 103 Rejections of the Claims

The Examiner rejected claims 1, 2, 8 - 10, 26 and 31 under 35 U.S.C. § 103(a) as being unpatentable over Caputo et al., U.S. Patent No. 5,778,071 (hereafter referred to as "Caputo"), in view of "The SSL Protocol Version 3.0" (hereafter referred to as the "SSL3spec"). Claims 1 and 26 are independent.

The Examiner rejected claims 1 and 26, in part, on the grounds that since Caputo mentions passing data in a single pass, it would have been obvious to pass non-pre-padded network security protocol data (taught by SSL3spec) in a single pass. However, as noted in Applicant's previous response, the conventional teaching was to process non-pre-padded network security protocol data in multiple passes. As explained at pages 3 and 9 of Applicant's specification and quoted in

Applicant's previous response, cryptographically processing non-pre-padded network security protocol data conventionally involved multiple processing steps. Hence, multiple passes across, for example, a PCI bus have been used to process the data.

None of the cited references address this issue. Neither Caputo nor Kaplan addresses processing non-pre-padded network security protocol data. Caputo discusses DES, MAC, DSA and RSA data. Kaplan discusses DES, SHAD-1 and MD5 data. The SSL3spec does not address the multiple pass problems. In view of the conventional practice in the art and the failure of the cited references to suggest that the issues involved in that conventional practice may avoided, there was no teaching that non-pre-padded network security protocol data may be passed in a single pass as claimed.

Applicant thus submits that independent claims 1 and 26 and claims 2 - 10 and 27 - 45 that depend on claim 1 or claim 26 are not obvious in view of the cited references. Moreover, the dependent claims are patentable over the cited references for the additional limitations that they contain. For example, claim 32 recites, in part, that data "is aligned into rows of data where each row of data contains a single type of data." In contrast, Caputo only teaches converting serial data to parallel data.

Claim 33 recites, in part: "aligning, for encryption operations, at least a portion of the received non-pre-padded network security protocol data and the authenticated at least a portion of the aligned network security protocol data to provide

the aligned network security protocol data for the encryption operations." Kaplan does not teach the claimed aligning at column 39 as cited by the Examiner. Kaplan makes no mention of aligning data after it has been authenticated.

Claim 41 recites, in part: "aligning and padding the non-pre-padded network security protocol data on the chip to enable the non-pre-padded network security protocol data to be passed in a single pass." There was no teaching or suggestion in the art that by aligning and padding non-pre-padded network security protocol after the data was received on the cryptography processing chip that it may be possible to pass the data in a single pass.

Claim 42 recites, in part: "the non-pre-padded network security protocol is passed across a non-dedicated data bus in a single pass." In contrast, Caputo is directed to a system where data is passed between the system 10 and a computer 22 via a dedicated connection 12 (see Figure 3). Hence, one skilled in the art addressing a problem that may be solved by claim 42--improved performance on a non-dedicated bus--would not be motivated to look to the teachings of Caputo since Caputo is not concerned with and does not address performance problems on a non-dedicated bus. Accordingly, one skilled in the art would not have been motivated to combine Caputo with the other references. As such claim 42 is not obvious in view of the cited references.

Claim 43 recites, in part: "receiving all SSL packet portion by the chip, padding and aligning the packet portions, cryptographically processing the packet portions and outputting

the cryptographically processed packet portions from the chip in a single pass over a data bus." There was no teaching or suggestion in the art to perform all of the operations recited here in a single pass.

Claims 44 and 45 recite, in part: "authentication data generated by the authentication component is passed to the encryption component and aligned by the encryption component" and "decrypted data generated by the encryption component is passed to the authentication component and aligned by the authentication component," respectively. None of the cited references teach or suggest that data processed by one cryptography component may be passed to another cryptography component then aligned as claimed. As discussed above, Kaplan does not teach the claimed aligning at column 39. Kaplan makes no mention of aligning data after it has been authenticated or decrypted.

CONCLUSION

For the foregoing reasons Applicant submits that the claims are patentable over the references of record. Reexamination and reconsideration are respectfully requested.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____

Stephen D. Burbach
Reg. No. 40,285
626/795-9900

SDB/vsj
SDB PAS646531.1-*-11/30/05 10:13 PM